REMARKS

The (new) Section 101 rejections of Claims 1-11 and 26-35 based on the allegation that these claims formerly recited only collecting information has been overcome, since Claims 1 and 26 now both require using at least the message point "x" and lattice point "y", digitally signing an entity.

Claims 1, 2, 12, and 26 (of which Claims 1, 12, and 26 are independent) have been rejected under 35 U.S.C. §102 as being anticipated by Goldreich et al., and dependent Claims 3-5, 9, 10, 13-18, 27-29, 31, and 33-35 have been rejected under 35 U.S.C. §103 as being unpatentable over Goldreich et al. in view of Diffie-Hellman. Contrary to the rejections that formed the basis of the prior appeal, Claims 6-8, 30, and 32 now have been indicated as reciting allowable subject matter and Claims 19-25, which includes independent Claim 19, now have been allowed.

To overcome the rejections, the subject matter of allowable Claim 6 has been moved into Claim 1, while the subject matter of allowable Claim 32 has been moved into independent Claim 26. Various claim cancellations and dependency amendments have been made to comport with the amendments to Claims 1 and 26. Accordingly, only independent Claim 12 remains at issue.

Anticipation Rejections Under 35 U.S.C. 102

Among other things, Claim 12 requires the message point "x" to be a point of a grid or a point of an auxiliary lattice, and finding a point "y" of a key lattice $\mathfrak{L}$ that is not the same as the auxiliary lattice. The rejection alleges that Section 3.3.2 of the primary reference teaches this, but this is incorrect. Section 3.3.2

teaches two presumably independent ways to decide on a distribution according to which a private basis is selected: using either a random lattice, or using a rectangular lattice. Section 3.3.2 does not appear to indicate any way in which both are used. Thus, the relied-upon portion teaches first establishing a lattice dimension, and then using one of two distributions for the single lattice, namely, ***either*** random ***or*** rectangular – but not that a message point "x" or a point "y" are part of either, much less that "x" and "y" are used as a digital signature. Not surprisingly, given that the primary reference does not appear to suggest two lattices in combination in the first place, the relied-upon sections fail to say anything about a point in one lattice (the auxiliary lattice, in Claim 12) being a map destination of a message and a point in another lattice ("key lattice") being used with the point in the first lattice, much less being used in combination with the other point as a digital signature.

This has been responded to with a partially correct if irrelevant reading of Claim 12. It is indeed correct that, as observed by the examiner, the message point "x" may be a point on a grid ***or*** on an auxiliary lattice. However, what has been left unexplained in the rejection is (1) what is the message point "x" in the relied-upon Section 3.3.2; (2) what is the corresponding grid or auxiliary lattice of which "x" is a point; (3) what is the point "y" in Section 3.3.2; (4) what is the corresponding key lattice from which "y" is selected; and (5) where the reference teaches that both the identified "x" and "identified "y" are used in a digital signature (page 18, section 5 has been identified but it does not appear to mention the specific points recited in Claim 12). As it stands, all that has been identified in the reference are a couple of seemingly independent lattices used for apparently different purposes without identifying all claim elements with any specificity in the reference.

Obviousness Rejections Under 35 U.S.C. 103

Nowhere does the primary reference mention the equivalency of its pre-map hash to any other means for rendering infeasible mapping two messages close together, much less that it can be replaced by Diffie-Hellman, much less still how such a wholesale revision might be made or what likelihood of success it would have, see MPEP §2143. Likewise, the secondary reference discusses the Diffie-Hellman algorithm but not in the context of a replacement for anything, much less as a replacement in a lattice-based system. Diffie-Hellman does not even appear to recognize the concept of "lattice". The only proferred Office Action rationale for combining the two references finds no citation in the references themselves, rendering the *prima facie* case against the dependent claims deficient.

Respectfully submitted,

John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg